IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA Plaintiff,	§ § §	
v.	§	NO: 6:24-CV-00027
$698,230.00 IN UNITED STATES CURRENCY Defendant.	§ § §	

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) and have been so employed since September 2001. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law

enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning $698,230.00 in Cathay Bank account 01749811 (Target Account), Check No. 2071007890 seized on or about October 30, 2023 in Plano, Texas pursuant to a seizure warrant.

LEGAL AUTHORITY FOR FORFEITURE

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to United States-based victims, including victims located in Tyler, Texas, which is located in the

Eastern District of Texas. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims' money.

5. This type of scam is often identified as "pig butchering" (derived from the Chinese phrase, which is used to describe this scheme) and involves scammers spending significant time getting to know, targeting and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH, or USDC deposit address, and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the "placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the "integration" phase is when these funds are then used to

promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 or a conspiracy to commit such offense.

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or a conspiracy to commit such is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept.

FACTS SUPPORTING FORFEITURE

14. The United States is investigating a pig butchering scheme involving a fraudulent cryptocurrency investment scheme that utilizes spoofed domains. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from pig butchering victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of the pig butchering victims. The Elights Trading Inc. bank account was provided to victims located within the Eastern District of Texas as a means in which they would pay their "taxes and/or fees" concerning their "earnings" as part of this scheme.

16. Investigation and review of the bank records for the Elights Trading bank account identified several additional victims who did send funds to the Elights Trading account as a result of this fraud scheme. Interviews with these victims identified additional bank accounts that received proceeds of this fraud scheme. One of these accounts was identified as the **TARGET ACCOUNT** held in the name of LSM TRADE LIMITED.

TARGET ACCOUNT INFORMATION AND TRANSACTIONS

17. Investigators obtained the bank records for the Cathay Bank account in the name of LSM Trade Limited, account number ending in 9811, the **TARGET ACCOUNT**. These bank records identified the signor on this account is identified as Shiming Li who presented a China passport as identification under EA0321946. The records indicate that on or about July 26, 2023, Shiming Li opened the business bank account identifying LSM Trade Limited as a corporation. The records reflect that Li provided the business address of 20 Confucius Plaza 44C, New York, New York 10002.

18. USSS investigators queried law enforcement databases regarding the identifiers utilized by Li to open the **TARGET ACCOUNT**. These queries included travel history and border crossings into the United States and no positive matches were readily identifiable. These results indicate the information provided by Li is fictitious and/or Li entered into the United States by other means.

19. Analysis of the bank records for the **TARGET ACCOUNT** indicate the following wire deposits were made into Target Account 1 totaling $1,830,764:

REMITTER/VICTIM	DATE	PAYMENT INFO
L.H	9/8/2023	$300,088
S.H	9/8/2023	$300,088
K.L.	9/11/2023	$11,888
M.Y.	9/11/2023	$80,000
C.J.	9/11/2023	$80,000
B.L.	09/14/2023	$25,000
Z.G.	9/15/2023	$50,000
T.P.	9/15/2023	$100,000
A.J.	9/19/2023	$23,000

E.C.	9/19/2023	$90,000
M.F.	9/20/2023	$40,000
J.D.	9/20/2023	$61,000
I.R.	9/20/2023	$100,500
J.M.	9/21/2023	$60,000
K.M.	9/22/2023	$20,000
J.D. (**2nd wire**)	9/25/2023	$60,000
A.J. (**2nd wire**)	9/26/2023	$21,000
G.M.	9/26/2023	$25,000
J.D. (**3rd wire**)	9/26/2023	$53,200
T.G.	9/26/2023	$270,000
E.O.	9/28/2023	$60,000

INTERVIEWS OF VICTIMS THAT SENT FUNDS TO THE TARGET ACCOUNT

20. Investigators interviewed additional victims who were identified as having sent funds to the **TARGET ACCOUNT** as a result of a cryptocurrency investment fraud scheme.

Victim B.L.

21. Investigators interviewed victim B.L. who confirmed his transaction of $25,000.00 to the **TARGET ACCOUNT** he sent on September 14, 2023. B.L. met someone online using the name Alice Chow. B.L. said his wife is terminally ill and as a result has been dealing with personal and financial hardships. B.L.'s conversation with Chow turned to investments in cryptocurrency in the spring of 2023. Chow introduced B.L. to a platform he believed was the exchange Coinone, where B.L. was able to establish an account and monitor his balance. B.L. was made to believe that he could fund his newly created account by wire transfer or by sending cryptocurrency to the

account and using it to buy options into unknown cryptocurrency coins. B.L. provided a screenshot of the account information for the **TARGET ACCOUNT**:

22. In addition to the wire transaction to the **TARGET ACCOUNT**, B.L. also sends funds from his bank account to his cryptocurrency account at crypto.com. B.L. explained that once his funds are credited to his crypto.com account, he converts them to Ethereum (ETH) and then sends funds to an address provided by Chow. B.L. stated once his funds are credited to what he believed was his Coinone account, he converted the ETH to Tether (USDT) for its stability. Then he was given a pyramid schedule of investments, noting that the more he was willing to invest, the greater his return on his investment would be. One of B.L.'s last transactions involved him sending ETH to what he thought was his Coinone account, using an address provided to him by Chow,

0x0FA0a0C1b30970c6ce50d57442e5D7A64Da0E78e, herein after known as E78e. B.L provided a screenshot of the wallet address he received from Chow:

23. Analysis of E78e by USSS investigators indicates that at no time during the reported transaction history of E78e did funds go directly from Crypto.com to Coinone, indicating the funds were not credited to B.L.'s Coinone account as he was made to believe.

24. B.L. has lost $241,435.00 as a result of this investment fraud scheme.

Victim I.R.

25. USSS investigators identified and interviewed victim I.R. regarding her transaction of $100,500 to the **TARGET ACCOUNT** on September 20, 2023. I.R. received a random text message from Lynne LNU, telephone number 213.423.1408, asking if she was available the next day for a job interview. Even though I.R. informed Lynne LNU that he had the wrong number, they continued to communicate and I.R. communicated daily with Lynne LNU and developed a relationship. After a few months of communications, I.R.'s discussion with Lynne LNU turned to investments into gold and how he is able to earn a great return on his investment. I.R. stated that Lynne LNU claimed that he has been using the platform CoinW (cglobalw.com) for years and there is a whole team who looks at the data to forecast when to trade gold. I.R. was skeptical of investing but eventually sent $100,500 to the **TARGET ACCOUNT**. I.R. questioned Lynne LNU about the legitimacy of the CoinW site. According to I.R., Lynne informed her they have many customers and they can guarantee that her funds will be returned to her.

26. USSS investigators identified the legitimate CoinW website is www.coinw.com, indicating that the domain I.R. was sent by Lynne LNU was spoofed.

27. I.R. told USSS investigators that upon her attempt to withdraw her funds, Lynne LNU informed her that "her account was suspected of money laundering" and that "the US regulatory authorities require them to close (I.R.'s) account as they are a regulated and formal trading platform." I.R. explained how CoinW customer service

advised her she could open a new account and have the funds from her old account transferred to her new account, where she would be able to withdraw her funds. According to I.R., the CoinW customer service reps said this process would "verify her source of legal funds."

28. I.R. confirmed that she believed she was investing only in gold. However, I.R. provided a screenshot image of a transaction to USSS investigators that reflected a transaction on September 14, 2023, that I.R. described as Lynne LNU depositing what appeared to be $100,500.98 USDC into her account, that was sent to 0x09F0c3DF403a95402B328EF68bfc4AC9B99F7921 (F7921). This was identified as an Ethereum (ETH) wallet address that received approximately $5 on September 14, 2023. This analysis suggests that the screen shot image provided to I.R. by Lynne LNU was fictitious.

29. USSS investigators reviewed the transaction details for wallet F7921. These details suggest that there were no funds in this transaction history being sent to the legitimate exchange CoinW, the exchange I.R. was made to believe she held an account at. This fact also suggests that the domains in this investigation are being spoofed and manipulated by unknown subjects, to make it appear the victims' accounts are increasing in value each time they send funds to a shell company or wallet from their handler/fraudster.

Victim Z.G.

30. USSS investigators identified and interviewed victim Z.G. regarding the $50,000 transaction he sent to the **TARGET ACCOUNT** on September 15, 2023. Z.G. he purchased $10,000 of Bitcoin, BTC, using his account at Coinbase in August 2023. Z.G. told USSS investigators that he thought his Coinbase account was hacked and/or compromised, however, he was able to recover most of his funds from this incident. After this incident, a friend introduced Z.G. to an uknown subject who attempted to persuade Z.G. to invest in cryptocurrency. Given his recent experience with Coinbase, Z.G. was of the opinion that investing in cryptocurrency was not safe. Z.G. explained that the individual was also seeking investors for his unknown hardware business. Z.G. stated that with an investment of $50,000 as a short-term loan, Z.G. was promised his funds back plus additional earnings of $5,000. Z.G. told USSS investigators that the unknown subject provided him the bank account details for the **TARGET ACCOUNT** as the avenue in which his investment would be utilized to invest in door hinges. Z.G. has not received any funds from his investment or any door hinges.

Victim T.P.

31. USSS investigators identified and interviewed victim T.P. regarding the $100,000 transaction he sent to the **TARGET ACCOUNT** on September 15, 2023. T.P. met a friend online, Tom LNU, who sent him an email regarding investing in a platform identified as Osmosis. T.P. was made to believe that Osmosis was a company that would house his investment account, where he would be able to view and access his account

online. T.P. has invested approximately $750,000 and is made to believe his account is holding approximately $3,500,000. T.P. attempted to retrieve a larger sum out of his account on or about September 30, 2023 when he was informed he would need to pay a 5% short term capital gains tax on his earnings ($2.8m), which equated to $140,000. T.P.'s Osmosis account has been inaccessible since his attempted withdrawal.

Target Account Transaction Activity

32. Investigators obtained bank records regarding the **TARGET ACCOUNT** and discovered that between September 12, 2023 to September 28, 2023, the withdrawal activity included bank fees and ten outgoing wire transactions. These wire transactions were sent to financial institutions in China and Singapore totaling $2,471,740.00.

33. The records for the **TARGET ACCOUNT** also indicate the recent victims sent a total of $1,830,764 to the **TARGET ACCOUNT** during the time period of September 8, 2023 – September 28, 2023.

34. During this time period, there were no identifiable normal business transactions such as payroll, utilities or other operational expenses for LSM Trade Limited.

35. Based on my training and experience, fraudsters will obtain business bank accounts to receive funds from victims based in the United States and rapidly move funds to places outside of the United States to avoid detection and seizure by law enforcement officers. This activity coupled with the rapid movement of funds reflected in the

transaction history of the **TARGET ACCOUNT** points to money laundering activity that is common in these fraud schemes.

36. On or about October 12, 2023, investigators provided a freeze letter request to Cathay Bank for assets and monies in the **TARGET ACCOUNT** to be frozen. Cathay Bank employees informed investigators that the **TARGET ACCOUNT's** balance is approximately $698,230.00.

37. On or about October 18, 2023, USSS investigators obtained and served a federal seizure warrant for any and all funds up to $698,230.00 held in the **TARGET ACCOUNT.**

38. On or about October 30, 2023, USSS investigators received a Cathay Bank cashier's check bearing number 2071007890 that was drawn on the **TARGET ACCOUNT** in the amount of $698,230.00.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $698,230.00 seized from Cathay Bank account 01749811in the name of LSM TRADE LIMITED.

40. Based on my experience and the information herein, I have probable cause to believe that the seized $698,230.00 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

41. The seized property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is personal property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957, or any property traceable to such property, and pursuant to 18 U.S.C. § 981(a)(1)(C) because it is personal property which constitutes or is derived from proceeds traceable to a violation of any offense constituting a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7)), namely, a violation of 18 U.S.C. § 1343, or a conspiracy to commit such offense (18 U.S.C. § 1349).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Brad Schley, Special Agent
U.S. Secret Service